

Steven T. Lovett, OSB No. 910701
steve.lovett@stoel.com
Rachel C. Lee, OSB No. 102944
rachel.lee@stoel.com
STOEL RIVES LLP
760 SW Ninth Avenue, Suite 3000
Portland, OR 97205
Telephone: 503.224.3380
Facsimile: 503.220.2480

Daniel F. Katz (*pro hac vice*)
dkatz@wc.com
David S. Kurtzer-Ellenbogen (*pro hac vice*)
dkurtzer@wc.com
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
Telephone: 202.434.5000
Facsimile: 202.434.5029

Attorneys for Defendant Intel Corporation

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON
PORTLAND DIVISION

In re INTEL CORP. CPU MARKETING,
SALES PRACTICES AND PRODUCTS
LIABILITY LITIGATION

Case No.: 3:18-md-2828-SI

This Document Relates to All Actions

DEFENDANT INTEL CORPORATION'S
MOTION FOR RECONSIDERATION,
OR, IN THE ALTERNATIVE, MOTION
TO CERTIFY PURSUANT TO 28 U.S.C.
§ 1292(b)

Oral Argument Requested

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
LR 7-1 CERTIFICATION	1
MOTION.....	1
LEGAL MEMORANDUM	1
INTRODUCTION	1
STANDARD OF REVIEW	6
ARGUMENT	8
I. THE COURT ON RECONSIDERATION SHOULD HOLD THAT THE NEW EXPLOITS THEORY FAILS TO STATE A PLAUSIBLE CLAIM.	8
A. Plaintiffs Cannot Base the Exploits Theory on Misrepresentations or Omissions.....	9
1. Plaintiffs’ Alleged Misrepresentations Under the Exploits Theory Are Not Actionable.	10
2. To the Extent the Exploits Theory Turns on Omissions, Plaintiffs Allege No Central Functional Defect.	11
B. Plaintiffs Have Not Stated a Non-Fraud Claim Under the Exploits Theory Either.....	12
1. California law requires a misrepresentation, physical safety hazard, or breach of warranty for product-based UCL unfair prong claims, none of which Plaintiffs allege.	13
2. Plaintiffs have not plausibly pled that Intel manipulated the Spectre and Meltdown embargo period.	15
3. Plaintiffs have failed to state a claim under the balancing test.	20
C. The Court Should Clarify That Claims Under the Exploits Theory May Not Proceed as to Purchases After the Widespread Disclosure of Spectre and Meltdown.	22
II. IN THE ALTERNATIVE, THE COURT SHOULD CERTIFY THE ORDER FOR APPEAL.	26
A. The Court Should Certify Whether the Lack of a Misrepresentation, Physical Safety Hazard, or Breach of Warranty Precludes Stating a Plausible Claim of Unfairness Here.....	27
B. The Court Should Certify Whether the Failure To Terminate an Embargo After a “Typical” Period States a Plausible Claim of Unfairness.....	29
CONCLUSION.....	30

TABLE OF AUTHORITIES

FEDERAL CASES

<i>A.H.D.C. v. City of Fresno, Cal.</i> , 2003 WL 25948686 (E.D. Cal. Mar. 3, 2003)	7
<i>Abarca v. Merck & Co.</i> , 2012 WL 137749 (C.D. Cal. Jan. 17, 2012)	7
<i>Adidas Am., Inc. v. TRB Acquisitions LLC</i> , 2018 WL 10335706 (D. Or. Nov. 8, 2018)	7
<i>Ahern v. Apple Inc.</i> , 411 F. Supp. 3d 541 (N.D. Cal. 2019)	9
<i>Allied Prof'l. Ins. Co. v. Anglesey</i> , 2018 WL 6219920 (C.D. Cal. June 14, 2018)	26
<i>Arizona v. Ash Grove Cement Co.</i> , 459 U.S. 1190 (1983)	28
<i>Arthur v. Murphy Co.</i> , 2012 WL 13047758 (D. Or. Jan. 17, 2012)	7, 8, 28, 30
<i>Boris v. Wal-Mart Stores Inc.</i> , 35 F. Supp. 3d 1163 (C.D. Cal. 2014)	10
<i>City of Los Angeles, Harbor Div. v. Santa Monica Baykeeper</i> , 254 F.3d 882 (9th Cir. 2001)	6
<i>Clemens v. DaimlerChrysler Corp.</i> , 534 F.3d 1017 (9th Cir. 2008)	15, 27
<i>E.E.O.C. v. Fred Meyer Stores, Inc.</i> , 954 F. Supp. 2d 1104 (D. Or. 2013)	7
<i>Gerritsen v. Warner Bros. Ent. Inc.</i> , 112 F. Supp. 3d 1011 (C.D. Cal. 2015)	19
<i>Greenspan v. Fieldstone Fin. Mgmt. Grp.</i> , 2018 WL 6682995 (D. Or. Dec. 18, 2018)	6
<i>Hauck v. Advanced Micro Devices, Inc. (Hauck I)</i> , 2018 WL 5729234 (N.D. Cal. Oct. 29, 2018)	23
<i>Hauck v. Advanced Micro Devices, Inc. (Hauck II)</i> , 2019 WL 1493356 (N.D. Cal. Apr. 4, 2019)	5, 24, 30
<i>Hauck v. Advanced Micro Devices, Inc. (Hauck III)</i> , 816 F. App'x 39 (9th Cir. 2020)	<i>passim</i>
<i>Hien Bui v. Mercedes-Benz USA</i> , 2021 WL 242936 (S.D. Cal. Jan. 25, 2021)	13
<i>Hodsdon v. Mars, Inc.</i> , 891 F.3d 857 (9th Cir. 2018)	14, 20
<i>ICTSI Oregon, Inc. v. Int'l Longshore & Warehouse Union</i> , 22 F.4th 1125 (9th Cir. 2022)	27
<i>In re Actimmune Mktg. Litig.</i> , 2010 WL 3463491 (N.D. Cal. Sept. 1, 2010)	9-10

<i>In re Century Aluminum Co. Sec. Litig.</i> , 729 F.3d 1104 (9th Cir. 2013)	20
<i>In re Cement Antitrust Litig. (MDL No. 296)</i> , 673 F.2d 1020 (9th Cir. 1981)	28
<i>In re Sony Grand WEGA KDF-E A10/A20 Series Rear Projection HDTV Litig.</i> , 758 F. Supp. 2d 1077 (S.D. Cal. 2010)	15
<i>Khoja v. Orexigen Therapeutics, Inc.</i> , 899 F.3d 988 (9th Cir. 2018)	18
<i>Klein v. Ljubljana Inter Auto d.o.o.</i> , 2021 WL 6424917 (C.D. Cal. Sept. 13, 2021)	13
<i>Natkin v. Am. Osteopathic Ass’n</i> , 2017 WL 4020425 (D. Or. July 27, 2017)	7
<i>Oestreicher v. Alienware Corp.</i> , 322 F. App’x 489 (9th Cir. 2009)	13
<i>Reese v. BP Expl. (Alaska) Inc.</i> , 643 F.3d 681 (9th Cir. 2011)	28, 29, 30
<i>Rote v. Comm. on Jud. Conduct & Disability</i> , 2021 WL 6197041 (D. Or. Dec. 30, 2021)	16
<i>Schedler v. FieldTurf USA, Inc.</i> , 2017 WL 8948593 (D. Or. Oct. 16, 2017)	7
<i>Smith v. Clark Cnty. Sch. Dist.</i> , 727 F.3d 950 (9th Cir. 2013)	6
<i>Steffler v. Williams</i> , 2010 WL 3122853 (D. Or. Aug. 9, 2010)	6
<i>Taleshpour v. Apple Inc.</i> , --- F. Supp. 3d ---, 2021 WL 3037703 (N.D. Cal. July 19, 2021)	14
<i>Talk Radio Network Enters. v. Cumulus Media Inc.</i> , 271 F. Supp. 3d 1195 (D. Or. 2017)	16
<i>Williams v. Apple, Inc.</i> , 449 F. Supp. 3d 892 (N.D. Cal. 2020)	9

STATE CASES

<i>Bardin v. DaimlerChrysler Corp.</i> , 39 Cal. Rptr. 3d 634 (Ct. App. 2006)	<i>passim</i>
<i>Cel-Tech Commc’ns, Inc. v. L.A. Cellular Tel. Co.</i> , 873 P.2d 527 (Cal. 1999)	14
<i>Daugherty v. American Honda Motor Co.</i> , 51 Cal. Rptr. 3d 118 (Ct. App. 2006)	13, 14, 15
<i>Seely v. White Motor Co.</i> , 403 P.2d 145 (Cal. 1965)	14

STATUTES AND RULES

6 U.S.C. § 659(m)	17
15 U.S.C. § 278g-3c(b)(1)	17, 22
28 U.S.C. § 1292(b)	<i>passim</i>

Fed. R. App. Proc. 5(a)(3)	26, 27
Fed R. Civ. Proc. 54(b)	6
Fed. R. Evid. 201(b)	19
LR 7-1(a)	1

OTHER AUTHORITIES

William B. Rubenstein, <i>The Concept of Equality in Civil Procedure</i> , 23 Cardozo L. Rev. 1865 (May 2002).....	26
---	----

LR 7-1 CERTIFICATION

Pursuant to LR 7-1(a), undersigned counsel certifies that the parties discussed this motion in good faith via telephone on February 22, 2022, and were unable to reach a resolution.

MOTION

Defendant Intel Corporation respectfully moves the Court to reconsider portions of its January 26, 2022 Order (ECF 225 (the “Order”)) granting in part and denying in part Intel’s motion to dismiss Plaintiffs Second Amended Complaint (ECF 209, the “Complaint” or “2AC”). In the alternative, Intel respectfully requests that the Court certify the Order for immediate appellate review pursuant to 28 U.S.C. § 1292(b).

LEGAL MEMORANDUM

INTRODUCTION

Since 2018, and across all three consolidated complaints, Plaintiffs have maintained that every Intel processor produced since 2006 contains “Defects” that are inherently actionable. Plaintiffs have consistently cited Intel’s alleged conduct in the wake of Google Project Zero’s discovery of Spectre and Meltdown as evidence of the alleged harm caused by those “Defects,” *not* as an independent basis for liability. This distinction has been clear in each of Plaintiffs’ three complaints, as the Court observed at oral argument in December 2021:

When I read the complaint and the first amended complaint and the second amended complaint, I didn’t see this as a case that basically says when Intel got the paper disclosing the defect in 2017, they waited too long to make that information public. That’s not the way I’ve ever looked at this case.

Ex. 1 (12/9/21 Hr’g Tr.) 58.¹

¹ All exhibits are attached to the Declaration of Steven T. Lovett.

Plaintiffs’ counsel readily agreed: “[I]t’s *always been* this started – *this is a defect* that started in 2006.” *Id.*; *see also infra* n.3.² Indeed, during that argument, the Court expressly sought to clarify whether Plaintiffs were asserting a new theory of liability based on Intel’s conduct after learning about Spectre and Meltdown, explaining that “when I read your second amended complaint, it looks to me . . . like you’re complaining about things that Intel did or didn’t do starting in 2006,” but “[n]ow what I’m hearing [Plaintiffs] saying is, no, what this case is really about is what Intel did or didn’t do starting in roughly, give or take, the middle of 2017.” Ex. 1 (12/9/21 Hr’g Tr.) 43. In response, Plaintiffs’ counsel expressly disavowed that new theory, informing the Court, “you misunderstood”: “*So I’m going to be really clear. In 2006 when [Intel] made the design change to relax privilege checks . . . they should be held responsible for that design decision.*” Ex. 1 (12/9/21 Hr’g Tr.) 43; *see also* Ex. 2 (12/1/20 Hr’g Tr.) 13-14 (prior hearing; after the Court noted that the “mitigation really only started in 2017,” Plaintiffs’ counsel responded: “[O]ur allegation is that back in 2006 . . . that’s when the problem really occurred with these chips.”).

Despite Plaintiffs’ emphatic framing of this case throughout as pertaining to alleged “Defects” in Intel CPUs, the Court’s recent Order now permits claims to proceed on a new and different theory that, for the first time, views security vulnerabilities as a source of liability *independent* of Plaintiffs’ theory of supposed “Defects.” This new “Exploits Theory” posits that, while Intel is not liable for any sales of supposedly defective processors before September 1, 2017, Intel may be held liable for “unfair” or “unjust” conduct in connection with sales after the allegedly “typical” 90-day embargo period for Spectre and Meltdown ended on that date.

² Unless stated otherwise, emphasis is added and internal citations and quotations are omitted.

But Plaintiffs’ own allegations demonstrate that Plaintiffs do not (and cannot) plead a plausible claim under the Exploits Theory. The Exploits Theory has never been how the Court—or Plaintiffs themselves—viewed the case, and arguments addressing that theory have therefore never been fairly and fully presented.³ Intel respectfully submits that adoption of this new theory without consideration of those arguments has yielded certain clear errors in the Court’s Order, and that those errors have resulted in manifest injustice. Intel accordingly now moves for reconsideration of the Court’s Order or, alternatively, to certify that Order for appellate review, for the following reasons.

First, the core allegations the Court cited in permitting the Exploits Theory to advance—such as that Intel “made public misrepresentations about the effect of Spectre and Meltdown on Intel processors,” Order at 22—sound in fraud. Permitting Plaintiffs to proceed with an unfairness claim that rests on such allegations is inconsistent with the Court’s correct reasoning in dismissing Plaintiffs’ other fraud-based claims, including the unfairness claim under the Defects Theory. Order at 15-16, 19-21; *see infra* Section I.A. The allegation that Intel manipulated an embargo period is also nothing more than an alleged omission—that “Intel could have disclosed Spectre and Meltdown sooner” but did not, Order at 23—and allowing that claim in the absence of a central

³ This MDL has always contained allegations about the vulnerability embargo and variants after Spectre and Meltdown, and the current Complaint is no different. But until now, the Court and Plaintiffs themselves have always viewed this case as addressing whether Intel’s allegedly defective designs dating to 2006 may subject Intel to liability, and have always viewed the new class of exploits discovered in 2017, and Intel’s conduct during the ensuing embargo, as examples of harm traceable to the alleged “Defects,” and not as independent sources of liability. *E.g.*, ECF 115 ¶¶ 2, 245, 256, 266, 280-81, 283-93, 297, 303; ECF 183 ¶¶ 5, 8-9, 473, 543, 554, 571, 578, 614, 616; 2AC ¶¶ 599, 610, 627, 670, 672, 915; ECF 192 at 5; ECF 204 at 2 (“Plaintiffs allege that Intel knew for decades about certain design *defects* in its microprocessors *that created security vulnerabilities*[.]”).

functional defect likewise runs afoul of the Court’s earlier orders, as well as California law and Ninth Circuit precedent.

Second, even if the allegation of manipulating the embargo period does not sound in fraud, that allegation cannot support a claim of unfairness under the UCL for multiple reasons. Most fundamentally, that claim fails because Plaintiffs do not plead an actionable misrepresentation, physical safety hazard, or breach of warranty, as required for any product-based unfairness claim under *Bardin v. DaimlerChrysler Corp.*, 39 Cal. Rptr. 3d 634 (Ct. App. 2006), and similar cases. *See infra* Section I.B.1. Intel has cited these cases previously in response to Plaintiffs’ Defects Theory, but the Order does not address this controlling authority, nor how it likewise precludes the new Exploits Theory.

Third, even if *Bardin* is not dispositive, Plaintiffs’ speculation that Intel improperly manipulated the Spectre and Meltdown embargo period is wholly implausible under the facts alleged. *See infra* Section I.B.2. The facts alleged in the Complaint show that Intel did **not** control the embargo period, which was established through a coordinated vulnerability disclosure process involving many researchers and affected industry participants. The Complaint also offers no well-pled facts from which it can be inferred that the allegedly “typical” 90-day embargo period should apply to mitigating Spectre and Meltdown, an indisputably novel and complex class of exploits. Indeed, the Complaint alleges facts showing that the embargo was actually **not long enough**, accusing Intel of “rush[ing] . . . out” patches before they were ready. 2AC ¶ 707.

Fourth, even if the embargo-manipulation claim did not fail for all the foregoing reasons, that claim is precluded by the balancing test the Court has adopted to assess unfairness. *See infra* Section 1.B.3. ***The theory that a party may incur liability under the UCL for adhering to established practices for coordinated vulnerability disclosure has never before been sanctioned***

by any court. Allowing Plaintiffs’ Exploits Theory to proceed on that theory ignores all countervailing data security concerns posed by premature disclosure—concerns that have led the United States Government to endorse the type of coordinated disclosure protocol employed here. Indeed, the Court’s Order creates a catch-22 that threatens the entire technology industry and the data security of all users: Withhold disclosure in keeping with best practices for coordinated vulnerability disclosure but at the peril of unfairness claims from new purchasers under the new Exploits Theory here, or disclose information about vulnerabilities not fully addressed within 90 days, thus giving a head start to hackers, putting the public’s data at risk, and potentially inviting unfairness claims from *existing* users. Once the data security concerns posed by premature disclosure are accounted for, the balancing test resolves in Intel’s favor as a matter of law.

Finally, even if the Court declines to reconsider whether a claim should proceed under the new Exploits Theory, it should still clarify or reconsider whether claims may proceed with respect to purchases *after* the public revelation of Spectre and Meltdown in January 2018. *See infra* Section I.C. Intel respectfully submits that allowing such claims to proceed not only conflicts with the Court’s prior reasoning, Plaintiffs’ own allegations, and the Court’s limitation of the case to seven Named Plaintiffs who all purchased *before* January 2018, but also squarely conflicts with the conclusion reached on indistinguishable facts in *Hauck v. Advanced Micro Devices, Inc.* (*Hauck II*), 2019 WL 1493356, at *13 (N.D. Cal. Apr. 4, 2019), *aff’d*, 816 F. App’x 39 (9th Cir. 2020) (*Hauck III*).

For all these reasons, the Court should reconsider its adoption of the Exploits Theory as a basis for liability. Alternatively, if the Court declines reconsideration, it should certify the Order for immediate appeal. Two issues in this case—the broad applicability of the rule articulated in *Bardin* and the potential imposition of liability for participating in coordinated vulnerability

disclosure practices consistent with industry best practices and endorsed by the United States Government—merit consideration at the appellate level.

STANDARD OF REVIEW

Reconsideration of an interlocutory order is generally appropriate under Federal Rule of Civil Procedure 54(b) when a court “(1) is presented with newly discovered evidence, (2) committed clear error or the initial decision was manifestly unjust, or (3) if there is an intervening change in controlling law.” *Smith v. Clark Cnty. Sch. Dist.*, 727 F.3d 950, 955 (9th Cir. 2013). Clear error occurs when a court does not apply controlling precedent to the facts presented:

It is common for both trial and appellate courts to reconsider and change positions when they conclude that they made a mistake. This is routine in judging, and there is nothing odd or improper about it. A trial court may reconsider and reach a conclusion contrary to an earlier decision, and a paradigmatic example of when this should be done is when the court made its prior decision without considering the legal standards in a controlling opinion.

Id.

Although clear error, manifest injustice, or a failure to consider material facts all constitute grounds for reconsideration, rigid adherence to those categories is not required. As the Ninth Circuit has explained, “as long as a district court has jurisdiction over the case, then it possesses the inherent procedural power to reconsider, rescind, or modify an interlocutory order for cause seen by it to be sufficient.” *City of Los Angeles, Harbor Div. v. Santa Monica Baykeeper*, 254 F.3d 882, 885 (9th Cir. 2001); *see also Greenspan v. Fieldstone Fin. Mgmt. Grp.*, 2018 WL 6682995, at *1 (D. Or. Dec. 18, 2018) (granting reconsideration and reversing order where, “[t]hough the Court is not convinced that this case presents a clear error requiring reconsideration, the Court has the discretion to reconsider and modify its interlocutory orders to correct mistakes”); *Steffler v. Williams*, 2010 WL 3122853, at *1 (D. Or. Aug. 9, 2010) (granting reconsideration

based on “additional briefing because I want to get this issue right”). “Whether or not to grant reconsideration is committed to the sound discretion of the court.” *E.E.O.C. v. Fred Meyer Stores, Inc.*, 954 F. Supp. 2d 1104, 1128 (D. Or. 2013) (granting reconsideration based on reassessment of legal authority previously presented).

Under 28 U.S.C. § 1292(b), district courts are permitted to certify interlocutory orders for immediate appeal where the underlying order involves “(i) a ‘controlling question of law,’ as to which (ii) ‘there is substantial ground for difference of opinion,’ and (iii) immediate appeal might ‘materially advance the ultimate termination of the litigation.’” *Schedler v. FieldTurf USA, Inc.*, 2017 WL 8948593, at *2 (D. Or. Oct. 16, 2017) (quoting 28 U.S.C. § 1292(b)); *see also Adidas Am., Inc. v. TRB Acquisitions LLC*, 2018 WL 10335706, at *1 (D. Or. Nov. 8, 2018). Certification under Section 1292(b) is particularly appropriate “‘where decision of an interlocutory appeal might avoid protracted and expensive litigation.’” *Schedler*, 2017 WL 8948593, at *2.

“An issue is ‘controlling’” under the first requirement “‘if ‘resolution of the issue on appeal could materially affect the outcome of litigation in the district court.’” *A.H.D.C. v. City of Fresno, Cal.*, 2003 WL 25948686, at *3 (E.D. Cal. Mar. 3, 2003). As to the second requirement, that there be a substantial ground for difference of opinion, “the primary inquiry is the strength of the arguments in opposition to the challenged ruling.” *Natkin v. Am. Osteopathic Ass’n*, 2017 WL 4020425, at *3 (D. Or. July 27, 2017) (quoting *Abarca v. Merck & Co.*, 2012 WL 137749, at *7 (C.D. Cal. Jan. 17, 2012)), *report and recommendation adopted*, 2017 WL 4012959 (D. Or. Sept. 12, 2017). The third requirement focuses on whether resolution of the interlocutory issue is “likely to materially speed the termination of the litigation.” *Arthur v. Murphy Co.*, 2012 WL 13047758, at *3 (D. Or. Jan. 17, 2012). “This factor is linked to whether an issue of law is ‘controlling’ in that the Court should consider the effect of a reversal by the court of appeals on the management

of the case.” *Id.* Where a case involves “both individual and class action claims” and “only limited pre-certification discovery has taken place,” the argument for certification is more compelling. *Id.*

ARGUMENT

I. THE COURT ON RECONSIDERATION SHOULD HOLD THAT THE NEW EXPLOITS THEORY FAILS TO STATE A PLAUSIBLE CLAIM.

The Court permitted Plaintiffs’ UCL unfair prong claim and their unjust enrichment claim to proceed for purchases of Intel-based devices after September 1, 2017, based on allegations that Intel “manipulate[ed] the embargo period to a longer time than the normal 90 days”; “advertis[ed] the performance and security of products knowing they were uniquely defective and would require extensive mitigation that would affect performance”; charged “premium price[s]”; “misrepresented that the exploits affected all processors when most of them allegedly only affect Intel’s processors, misrepresented the negative effects of the mitigation, and intentionally suppressed testing and dissemination of test results of the effects of the mitigation.” Order at 22, 25. The Court should reconsider its holding on this new Exploits Theory for several reasons.

First, these allegations plainly sound in fraud, yet fail to state a claim for fraud by either affirmative misrepresentations or omission, for the same reasons the Court has already held in dismissing with prejudice *all* claims sounding in fraud. ECF 204 (3/29/21 Order) at 20.

Second, a UCL unfairness claim in the consumer product context requires an actionable misrepresentation, physical safety hazard, or breach of warranty, none of which is alleged here. The failure of the unfairness claim also dooms the California unjust enrichment claim.⁴

Third, even construing Plaintiffs’ allegation that Intel manipulated the embargo period as

⁴ Plaintiffs’ claim for unjust enrichment rests on the same allegations as their unfairness claim under the UCL, and fails for the same reasons: absent actionable unfair conduct by Intel, there is no basis to find “an unjust retention of benefits” by Intel. *See* Order at 25.

a conduct claim, rather than an omission claim (*but see* Order at 13 (summarizing the allegation as one that “Intel ***kept the security exploits a secret*** longer than a normal embargo”)), Plaintiffs have not pled facts sufficient to support a plausible allegation that Intel manipulated the embargo period; their allegations instead compel the contrary inference.

Fourth, even under the UCL balancing test, the benefits of avoiding the risks posed by premature disclosure of the vulnerabilities, before development of adequate patches, clearly outweigh—as a matter of law—the harm Plaintiffs allege.

Finally, the Court should expressly confirm that conduct after January 2, 2018 is not actionable, given the widespread publicity surrounding the disclosure of the new class of vulnerabilities at issue here (which includes all subsequent variants), given Plaintiffs’ refusal for the past two years to name anyone injured after that disclosure, and given the conclusion reached in *Hauck* with respect to a post-January 2018 purchaser.

Plaintiffs have always argued a Defects Theory to support their case, and in fact have strenuously disclaimed an Exploits Theory (until now). Considering Plaintiffs’ own allegations and controlling law, that new theory manifestly fails.

A. Plaintiffs Cannot Base the Exploits Theory on Misrepresentations or Omissions.

Because the new Exploits Theory is based on the notion that “Intel ***intentionally duped*** every purchaser of an Intel CPU since mid-2017,” 2AC ¶ 31, this new theory survives only if it meets the standards for pleading fraud. A claim of unfairness based on alleged misrepresentations or omissions must be dismissed if it does not state a claim for fraud. *See Williams v. Apple, Inc.*, 449 F. Supp. 3d 892, 910 (N.D. Cal. 2020) (misrepresentations); *Ahern v. Apple Inc.*, 411 F. Supp. 3d 541, 561 (N.D. Cal. 2019) (omissions); *In re Actimmune Mktg. Litig.*, 2010 WL 3463491, at *11 (N.D. Cal. Sept. 1, 2010) (dismissing unfair claim where “[o]ver and over again, plaintiffs

complain that defendants’ conduct was unfair because they knew that Actimmune was ineffective in treating IPF, but nonetheless represented to doctors and patients suffering from IPF that Actimmune could effectively treat IPF,” because “[s]uch allegations are quintessential examples of fraud”), *aff’d*, 464 F. App’x 651 (9th Cir. 2011). For the same reasons the Court already stated in connection with the Defects Theory, the Exploits Theory does not state a claim for fraud and therefore cannot support an unfair-prong claim either.⁵

1. Plaintiffs’ Alleged Misrepresentations Under the Exploits Theory Are Not Actionable.

In its Order, the Court recognized that Plaintiffs “do not allege that they heard any *actionable* representation by Intel relating to security, or even performance.” Order at 20 (emphasis in original). Nonetheless, it permitted claims to proceed under a new Exploits Theory principally based on Intel’s alleged misrepresentations during and after the 2017 Spectre and Meltdown embargo—including Intel’s advertising and its statements concerning Spectre and Meltdown and their mitigations—even though a misrepresentation claim that does not identify any actionable misrepresentation fails as a matter of law. *See* Order at 29 (dismissing state-law misrepresentation claims grounded in “only general statements about speed or performance” that are “not actionable as a misrepresentation”).

In permitting Plaintiffs to proceed on the Exploits Theory, the Court concluded that the new theory “does not entirely overlap with Plaintiffs’ UCL claim based on fraud,” which the Court had already rejected for the Defects Theory. Order at 15. But even if the new Exploits Theory is

⁵ Plaintiffs’ allegation of “premium pricing” cannot give rise to liability. Outside antitrust law and absent fraud, there is no basis for holding a party liable for charging “too high” a price. “[T]he price is simply the amount at which the merchant offers to sell the product . . . not a statement about the product.” *Boris v. Wal-Mart Stores Inc.*, 35 F. Supp. 3d 1163, 1169-70 (C.D. Cal. 2014) (dismissing UCL fraud and unfairness claims). Thus, a “[m]erchant’s liability cannot be premised solely on a consumer’s assumptions about a product based on a product’s price.” *Id.* at 1170.

not *the same fraud argument* that Plaintiffs previously asserted, it is nonetheless *a fraud argument*, and it fails to state a claim under the same principles that the Court already concluded bar Plaintiffs’ Defects Theory. As the Court has stated: “*Plaintiffs*, versus generic ‘buyers,’ need to allege that *they* saw or heard representations by Intel and relied on those representations to support the conclusion that Intel’s conduct was unfair.” Order at 19 (emphasis in original). The same holds true for the misrepresentations Plaintiffs allege regarding the new Exploits Theory, including supposed “public misrepresentations about the effect of Spectre and Meltdown on Intel processors, the fact that Intel’s chips were uniquely affected based on its designs, and the effect of the mitigation on performance.” Order at 22. Additionally, the Court’s rejection of Plaintiffs’ reliance on general statements about speed and performance in Intel’s advertising to support their Defects Theory applies equally to Plaintiffs’ attempt to rely on Intel’s “advertising the performance and security of products” before disclosure of the exploits and their mitigations (Order at 22): “Plaintiffs do not allege that *they heard* any actionable representation by Intel relating to security, or even performance.” Order at 19-20 (emphasis in original).

2. To the Extent the Exploits Theory Turns on Omissions, Plaintiffs Allege No Central Functional Defect.

The linchpin of the Exploits Theory is that “Intel could have disclosed Spectre and Meltdown sooner” but did not. Order at 23; *see also id.* (noting Plaintiffs’ theory rests on the “argument that consumers *were not given the full and accurate picture* after the public disclosure of Spectre and Meltdown”). That is plainly an omission claim. So too is Plaintiffs’ allegation that Intel “*suppressed*” information concerning “testing” and “the effects of the mitigation” both during and after the embargo. Order at 33; *id.* at 22-23, 25. But, just as the Court observed in connection with the Defects Theory, “Plaintiffs’ assertion of an omission-based unfair conduct UCL claim is simply a UCL fraud-by-omission claim.” Order at 15. And, as the Court found in its opinion on

Intel's prior motion to dismiss, Plaintiffs' UCL omissions claim fails because such a claim requires that undisclosed information "be *central* and important to the *product's function*," yet Intel chips have continued to "perform[] their central function." ECF 204 (3/29/21 Order) at 16-17 (emphasis in original); *see also Hauck III*, 816 F. App'x at 44 (plaintiffs failed to plausibly allege AMD processors were not fit for ordinary use). The Complaint adds nothing that could change that conclusion. Like the dismissed Defects Theory, there is still no allegation regarding the new Exploits Theory that Intel processors fail to perform their central function as processors, and millions of consumers continue to buy and use devices with Intel chips.

B. Plaintiffs Have Not Stated a Non-Fraud Claim Under the Exploits Theory Either.

Even construing Plaintiffs' allegations under the new Exploits Theory as alleging conduct that does not sound in fraud, Plaintiffs' attempt to state an Exploits Theory claim under the unfair prong of the UCL still fails for three reasons: (1) no such claim can proceed absent a misrepresentation, physical safety hazard, or breach of warranty; (2) Plaintiffs have not *plausibly* pled that Intel manipulated the embargo period, only that the embargo lasted longer than the allegedly "typical" 90 days; and (3) the facts alleged fail to state a UCL unfair prong claim under the balancing test the Court has adopted.

Reconsideration is appropriate because the Court and Plaintiffs alike have consistently viewed and presented this case as animated by a Defects Theory; the application of these principles to the Exploits Theory has never been the subject of the parties' briefing; and controlling law on these issues requires dismissal with prejudice of the Exploits Theory, too.

1. California law requires a misrepresentation, physical safety hazard, or breach of warranty for product-based UCL unfair prong claims, none of which Plaintiffs allege.

In numerous cases relating to consumer products—most notably *Bardin v. DaimlerChrysler Corp.*, 39 Cal. Rptr. 3d 634 (Ct. App. 2006), and *Daugherty v. American Honda Motor Co.*, 51 Cal. Rptr. 3d 118 (Ct. App. 2006)—California appellate courts have limited UCL unfair prong claims to situations involving a misrepresentation, physical safety hazard, or breach of warranty. *Bardin*, 39 Cal. Rptr. 3d at 643; *Daugherty*, 51 Cal. Rptr. 3d at 129-30. The Ninth Circuit has recognized and applied this rule. *See, e.g., Oestreicher v. Alienware Corp.*, 322 F. App'x 489, 493 (9th Cir. 2009) (“A manufacturer’s duty to consumers is limited to its warranty obligations absent either an affirmative misrepresentation or a safety issue.”).⁶ This governing rule requires dismissal of the Exploits Theory unfairness claim here, because Plaintiffs do not allege an actionable misrepresentation, a physical safety hazard, or a breach of warranty.

Although Intel previously cited these cases, it did so in the context of addressing the Defects Theory advanced by Plaintiffs. *See, e.g.,* ECF 213 (Intel MTD 2AC) at 31 (arguing against “unfair design choice” theories of liability). This is likely why the Court did not discuss the *Bardin* line of cases in its Order, having rejected the Defects Theory on other grounds. But these cases are equally relevant to the new Exploits Theory, and should be considered by the Court in that context before any final determination that Exploits Theory claims may advance.

Bardin built on the California Supreme Court’s seminal ruling that while “[a] consumer should not be charged at the will of the manufacturer with bearing the risk of *physical injury*,” the consumer *can* be “fairly charged with the risk that the product will not match his *economic*

⁶ *See also Klein v. Ljubljana Inter Auto d.o.o.*, 2021 WL 6424917, at *7 (C.D. Cal. Sept. 13, 2021) (same); *Hien Bui v. Mercedes-Benz USA*, 2021 WL 242936, at *3 (S.D. Cal. Jan. 25, 2021) (same).

expectations unless the manufacturer agrees that it will.” *Seely v. White Motor Co.*, 403 P.2d 145, 151 (Cal. 1965). *Bardin* also honored the California Supreme Court’s instruction that courts cannot invoke “amorphous” standards of unfairness that “provid[e] ‘too little guidance to courts and businesses,’” nor “simply impose their own notions of the day as to what is fair or unfair.” *Bardin*, 39 Cal. Rptr. 3d at 640 (quoting *Cel-Tech Commc’ns, Inc. v. L.A. Cellular Tel. Co.*, 873 P.2d 527, 543 (Cal. 1999)).

These principles apply broadly to all UCL unfair prong claims in the consumer product area, as subsequent cases applying *Bardin* and *Daugherty* expressly apply them outside the design-choice context. Most significantly, in *Hodsdon v. Mars, Inc.*, the Ninth Circuit relied on *Bardin* in holding that a party’s failure to disclose information about the alleged use of slave labor was not unfair where “it had no duty to disclose [the information] in the first place.” 891 F.3d 857, 867 (9th Cir. 2018); *see also Taleshpour v. Apple Inc.*, --- F. Supp. 3d ---, 2021 WL 3037703, at *6 (N.D. Cal. July 19, 2021) (“California federal courts have generally interpreted *Daugherty* as holding that ‘[a] manufacturer’s duty to consumers is limited to its warranty obligations absent either an affirmative misrepresentation or a safety issue.’” (alteration in original)), *appeal docketed*, No. 21-16282 (9th Cir. Aug. 5, 2021).

Here, the remaining seven Named Plaintiffs do not allege that the Intel CPUs they purchased after September 1, 2017 posed any physical safety hazard, nor that those CPUs failed to live up to any actionable promise by Intel. Notably, although Plaintiffs claim that, after installing mitigation patches, they did not receive the speed or performance that they anticipated, they do not allege (nor could they) that Intel warranted the CPUs would be free of vulnerabilities, would never require patches, or would provide a guaranteed level of speed or performance. California law is clear that a UCL unfair prong claim does not lie where a product functions as

warranted, but nevertheless fails to meet the purchaser's expectations. *See, e.g., Clemens v. DaimlerChrysler Corp.*, 534 F.3d 1017, 1026-27 (9th Cir. 2008) (UCL unfair prong claim failed where product performed as warranted); *In re Sony Grand WEGA KDF-E A10/A20 Series Rear Projection HDTV Litig.*, 758 F. Supp. 2d 1077, 1091 (S.D. Cal. 2010) (same); *Daugherty*, 51 Cal. Rptr. 3d at 130 (same). A claim that a manufacturer inflated its prices, such that the purchaser paid more than he otherwise would have, does not alter this rule: *Bardin* explicitly rejected the argument that Chrysler's profit motive in using inferior steel sufficed to state a UCL unfair prong claim. 39 Cal. Rptr. 3d at 643-44. Plaintiffs' claim that they paid a "premium" price for a product whose performance was not as "superior" as they expected is one of disappointed "economic expectations." *Id.* at 644. Under *Bardin* and *Daugherty*, such allegations cannot support a UCL unfair prong claim whether under the Defects Theory Plaintiffs have pressed since the outset of this litigation or under the new Exploits Theory.

2. Plaintiffs have not plausibly pled that Intel manipulated the Spectre and Meltdown embargo period.

Even if the *Bardin* line of cases did not bar the new Exploits Theory, that theory still fails because it turns on an allegation—Intel's supposed manipulation of the Spectre and Meltdown embargo period—that cannot plausibly be inferred from the facts pled.

While Plaintiffs allege that the Spectre and Meltdown embargo lasted longer than 90 days, their allegations also unequivocally establish that the length of the embargo was the result of a *coordinated process* involving researchers and industry participants adhering to the generally accepted best practice that public disclosure of a new vulnerability should come only after an effective mitigation is ready to be deployed. *See* Ex. 3 (Moritz Lipp et al., *Meltdown: Reading Kernel Memory from User Space* (2018) (cited 2AC ¶¶ 602-03, 607)) at 1 n.10 (noting that researchers agreed to embargo period "[i]n coordination with industry"). Thus, Plaintiffs have not

plausibly alleged that the embargo was extended beyond the “typical” 90 days *because of* “manipulation” by Intel.⁷ The Court should reconsider its creation of a new type of cause of action—for which there is no precedent—exposing technology companies to costly litigation for conducting ordinary sales and marketing activity while adhering to industry-standard coordinated vulnerability disclosure processes designed to protect consumers.

a. Plaintiffs’ Reliance on “Information and Belief” Does Not State a Plausible Claim That Intel Manipulated the Embargo Period.

Plaintiffs allege Intel’s supposed manipulation of the embargo only “on information and belief.” 2AC ¶ 539. But “[i]n the post-*Twombly* and *Iqbal* era, pleading on information and belief, without more, is insufficient to survive a motion to dismiss”; instead, “a pleading must be ‘plausibly suggesting (not merely consistent with)’ behavior to satisfy threshold pleading standards.” *Talk Radio Network Enters. v. Cumulus Media Inc.*, 271 F. Supp. 3d 1195, 1207 (D. Or. 2017) (dismissing claim that defendant was “manipulating payments contrary to vaguely described industry norms”). Thus, when alleging misconduct “on information and belief,” Plaintiffs cannot rely on “speculative, conclusory, and unsupported allegations,” but must allege *facts* to support their conclusion. *Rote v. Comm. on Jud. Conduct & Disability*, 2021 WL 6197041, at *13 (D. Or. Dec. 30, 2021).

⁷ This failure to plead a plausible claim of embargo manipulation constitutes a second, independent flaw in this new theory of liability. As discussed above, Plaintiffs cannot proceed on a theory resting on an alleged omission, but Plaintiffs’ own allegations make clear that the supposed embargo manipulation is nothing more than an alleged omission, i.e., a prolongation of the period in which Intel did not disclose the Spectre and Meltdown exploits. 2AC ¶ 915 (“Intel has manipulated the disclosure process and has *refused to disclose security vulnerabilities for much longer periods* despite knowing about them.”). The Order, too, reflects Plaintiffs’ characterization of the alleged manipulation as a form of omission. See Order at 13 (“Intel *kept the security exploits a secret* longer than a normal embargo[.]”).

Plaintiffs fail that threshold requirement. They reference an allegedly “typical” 90-day embargo period only twice in their 1,699-paragraph Complaint. 2AC ¶¶ 539, 915. But their own allegation makes clear that even that cursory reference to a “typical” period is tied to *software* vulnerabilities. 2AC ¶ 539. Plaintiffs do not allege that hardware and software vulnerabilities are comparable, such that the allegedly “typical” period for one is “typical” for the other. Plaintiffs’ own allegations also demonstrate that the Spectre and Meltdown vulnerabilities were anything but typical; those allegations thus preclude an inference that the “typical” 90-day embargo period should apply to the “extremely complicated” issues presented in the Spectre and Meltdown hardware mitigations.⁸ The degree of difficulty matters, as the purpose of embargoes is “to give vendors time to develop remediations without attackers also having access to public vulnerability information.” Ex. 7 (Int’l Org. for Standardization (“ISO”) / Int’l Electrotechnical Comm’n (“IEC”), ISO/IEC 29147 – *Information Technology – Security techniques – Vulnerability disclosure* (Oct. 2018) (“ISO 29147”)) at 12.⁹

Plaintiffs’ own allegations likewise rule out a plausible claim of unfairness based on the assertion that “Intel should have disclosed that there were pending security mitigations that could impact security and performance and provided approximate ranges that the mitigations could impact devices with Intel CPUs” in order to “remove[] the information asymmetry that Intel was

⁸ Plaintiffs’ own cited authorities describe how “hard to fix” and “extremely complicated” Spectre and Meltdown were. Ex. 4 (Adam Hastings and Simha Sethumadhavan, *WaC: A New Doctrine for Hardware Security*, ASHES ’20 (Nov. 13, 2020) (cited 2AC ¶ 539)) at 1; Ex. 5 (Computer Hope, *What Are Meltdown and Spectre?*) (cited 2AC ¶ 601)) at 3; Ex. 6 (Fortinet, *Meltdown/Spectre Update* (Jan. 30, 2018) (cited 2AC ¶ 688)) at 3.

⁹ ISO 29147, along with ISO 30111, are standards issued by the International Standards Organization and endorsed by Congress in connection with the federal government’s development of a coordinated vulnerability disclosure policy. *See* 15 U.S.C. § 278g-3c(b)(1); *see also* 6 U.S.C. § 659(m) (providing for development of coordinated vulnerability disclosure policies by the Department of Homeland Security).

exploiting to sell defective CPUs” during the embargo period. 2AC ¶ 555. As Plaintiffs’ own Complaint establishes, it is “[s]tandard practice” to set “an embargo date,” before which “**nobody does anything publicly**,” including “publish[ing] advisories.” Ex. 8 (Colin Percival, *Some Thoughts on Spectre & Meltdown*, Daemonic Dispatches Blog (Jan. 17, 2018 2:40 PM) (cited 2AC ¶ 574)) at 5 (emphasis in original). Plaintiffs cannot evade the dispositive impact of this rule, incorporated by reference in their Complaint. To the contrary, as the Ninth Circuit has made clear, “[t]he doctrine [of incorporation by reference] prevents plaintiffs from selecting only portions of documents that support their claims, while omitting portions of those very documents that weaken—or doom—their claims.” *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir. 2018).

b. No Well-Pled Facts Support a Plausible Inference that Intel Manipulated the Spectre and Meltdown Embargo Period.

It is undisputed that the embargo for Spectre and Meltdown extended beyond what Plaintiffs contend is the “typical” 90 days. But Plaintiffs proffer no facts from which to infer that the extended period was due to alleged “manipulation” by Intel rather than the need for additional time to ensure adequate mitigations were developed before public disclosure of this new class of exploits. To the contrary, Plaintiffs expressly allege that the actual embargo (from June 1, 2017, to January 3, 2018), while longer than 90 days, was still **not long enough** to develop market-ready mitigations: According to Plaintiffs, Intel had to “rush[] initial fixes out” after Spectre and Meltdown leaked, with the consequence that those initial patches “caused unacceptable data corruption and loss,” and even “resulted in disabled servers.” 2AC ¶ 707.¹⁰

¹⁰ As Plaintiffs’ citations confirm, AMD’s initial patches released after the premature disclosure on January 2, 2018, were glitchy too. Ex. 9 (Joe Osborne, *Don’t download Intel’s latest Spectre and Meltdown patch, Intel Warns*, TechRadar (Jan. 22, 2018) (cited 2AC ¶ 713)) at 8 (“AMD is suffering a similar fate[.]”).

Rather than offering *facts* supporting Intel’s alleged manipulation of the embargo period, Plaintiffs rely on speculation, positing that because Intel allegedly had a profit motive to delay disclosure of Spectre and Meltdown, it must therefore have manipulated the embargo period to increase its profits. 2AC ¶ 555. Once again, the materials Plaintiffs incorporated in the Complaint preclude such an inference, as they make clear that the length of the embargo was not set by Intel unilaterally, but rather was coordinated by “disjoint groups” of researchers such as Google Project Zero, “CPU vendors” (including Intel but also AMD, one of Intel’s principal competitors) and “other affected companies.”¹¹ Plaintiffs do not allege (nor could they) that independent researchers, “other affected companies,” or other “CPU vendors”—i.e., Intel’s direct competitors—had any motivation to assist Intel in increasing its profits. It is wholly implausible to infer that Intel manipulated the embargo period for Spectre and Meltdown to increase its profits when Plaintiffs’ own allegations show that the embargo period was agreed to by *all* participants,

¹¹ Ex. 3 (Lipp, et al.) (cited 2AC ¶¶ 602-03, 607) at 1 n.10. Such “coordinated vulnerability disclosure” (or “CVD”) is recognized as a best practice by state, federal, and international governments because it “reduces the risk associated with exploiting vulnerabilities.” Ex. 7 (ISO 29147) at 1 (explaining that “[c]oordinated vulnerability disclosure is especially important when multiple vendors are affected”); *see also* Ex. 10 (Ohio Secretary of State, *Vulnerability Disclosure Policy*) at 3 (adopting coordinated vulnerability disclosure policy because “disclosure in absence of a readily available remediation tends to increase risk rather than reduce it”); Ex. 11 (Cybersecurity & Infrastructure Security Agency, *Guide to Vulnerability Reporting for America’s Election Administrators*) at 3 (noting benefit of coordinated vulnerability disclosure is that it “help[s] the affected entity fix vulnerabilities before public disclosure”); Ex. 12 (Netherlands Nat’l Cyber Security Centre, Ministry of Justice and Security, *Coordinated Vulnerability Disclosure: the Guideline* (Oct. 2018)) at 7 (“In CVD, knowledge is shared with one or more potentially vulnerable organisations in order to arrive at a joint solution for the vulnerability found in collaboration with the reporting party. It is important that the organisations affected have sufficient time to remedy any vulnerabilities or protect systems in order to limit or prevent loss or damage as much as possible. The cornerstone of the process is disclosure of knowledge about the vulnerabilities after remediation.”). Intel requests that the Court take judicial notice of these ISO standards and government-issued documents. Fed. R. Evid. 201(b); *Gerritsen v. Warner Bros. Ent. Inc.*, 112 F. Supp. 3d 1011, 1033 (C.D. Cal. 2015) (“[T]he court can take judicial notice of . . . websites run by governmental agencies.”).

including Intel’s direct competitors such as AMD. For this reason, Plaintiffs’ allegations fail to support a plausible claim that Intel acted unfairly regarding the embargo. *See In re Century Aluminum Co. Sec. Litig.*, 729 F.3d 1104, 1108 (9th Cir. 2013) (explaining that, “[w]hen faced with two possible explanations, only one of which can be true and only one of which results in liability, plaintiffs cannot offer allegations that are merely consistent with their favored explanation but are also consistent with the alternative explanation”; instead, “[s]omething more is needed, *such as facts tending to exclude the possibility that the alternative explanation is true*, in order to render plaintiffs’ allegations plausible”).

3. Plaintiffs have failed to state a claim under the balancing test.

Embracing a bright-line rule regarding an allegedly “normal” embargo period—with failure to disclose after 90 days deemed plausibly unfair—fundamentally misapplies the UCL’s balancing test. That test, adopted by the Court (Order at 13), requires weighing the harm alleged by a plaintiff against the countervailing utility of a defendant’s conduct, and is often determined as a matter of law. *See Bardin*, 39 Cal. Rptr. 3d at 644 n.6 (dismissing under balancing test as a matter of law); *Hodsdon*, 891 F.3d at 867 (same); *Hauck III*, 816 F. App’x at 43 (same). Here, Plaintiffs’ own allegations show, as a matter of law, that the significant data security risks tied to premature disclosure of Spectre and Meltdown outweigh the disappointed expectations that the seven remaining Named Plaintiffs allege they suffered by purchasing Intel CPUs during the embargo.

In applying the balancing test to Plaintiffs’ claim, the Court concluded that, “[b]ased on Plaintiffs’ allegations, it is not clear that Intel had a countervailing business interest other than profit for delaying disclosure for as long as it did (through the holiday season), for downplaying the negative effects of the mitigation, for suppressing the effects of the mitigation, and for

continuing to embargo further security exploits that affect only Intel processors.” Order at 24.¹² The balancing test, however, is not limited to assessing a defendant’s business interests. Rather, as the Court noted, “[i]t requires a court to weigh *the utility of the defendant’s conduct* against the gravity of the harm to the alleged victim.” Order at 13.

Here, Plaintiffs’ own allegations unequivocally reveal the utility of the decision (which, per Plaintiffs’ allegations, was made by Intel *in conjunction with* a host of other industry and third-party participants) to extend the embargo to permit sufficient time for the various impacted parties (including Intel and AMD as well as other hardware and software manufacturers) to develop and implement mitigations for the Spectre and Meltdown exploits. The Complaint itself canvasses the parade of horrors that would allegedly result had Plaintiffs’ computers been left vulnerable to the “significant security threat” posed by Spectre and Meltdown absent mitigations. 2AC ¶¶ 15, 242-43, 252. Indeed, the new Exploits Theory expressly rests on the notion that users *prefer* to install the mitigations—despite the patches’ claimed inadequacies and their alleged impact on speed and performance—because otherwise they would be exposed to this alleged security threat. Accepting as true Plaintiffs’ allegation of a “significant security threat” arising from this new class of exploits, 2AC ¶ 15, that allegation fatally undermines any claim that it was “unfair” of Intel and other industry participants to coordinate disclosure of the exploits with the release of patches to protect against that same “significant security threat.” No reasonable Plaintiff

¹² Only the first allegation—that Intel “delay[ed] disclosure for as long as it did (through the holiday season)” —applies to Plaintiffs. The remaining allegations all relate to alleged conduct by Intel *after* the January 2018 disclosure of Spectre and Meltdown, and *after* all seven remaining Named Plaintiffs purchased the CPUs at issue here. 2AC ¶¶ 63, 106, 118, 257, 306, 330, 354. Plaintiffs have not alleged (and, given the timing of their purchases, could not allege) any basis to rely on purported misrepresentations or omissions by Intel that occurred months or years *after* their purchases.

or putative class member would have wanted Intel to unilaterally end the embargo prematurely, simply because 90 days had passed, and thereby put their data security at risk.¹³

In short, Plaintiffs’ own allegations show that the “information asymmetry” about which they complain, 2AC ¶ 539, was necessary to protect the public—including Plaintiffs—until patches were available to address the risks posed by Spectre and Meltdown. That is precisely why federal law endorses the international standards that caution against disclosure before a patch is ready, and that note that coordinated vulnerability disclosure “aim[s] to minimize risk, cost, and harm to all stakeholders”—including end users. *See* Ex. 7 (ISO 29147) at vii, 17, 20; Ex. 13 (ISO 30111) at 6, 11 (endorsed in 15 U.S.C. § 278g-3c(b)(1)). Therefore, Plaintiffs’ claim that Intel acted “unfairly” by not unilaterally terminating the embargo after 90 days does not (and cannot) plead a plausible claim of unfairness under the balancing test.

C. The Court Should Clarify That Claims Under the Exploits Theory May Not Proceed as to Purchases After the Widespread Disclosure of Spectre and Meltdown.

If the Court does not conclude that Plaintiffs’ UCL and unjust enrichment claims fail in their entirety for the reasons discussed above, it should nonetheless clarify or reconsider the part of the Order relating to Intel CPU purchases *after* the widespread public disclosure of Spectre and Meltdown in January 2018. That expanded scope cannot be squared with Plaintiffs’ deliberate and steadfast refusal to identify a single person who could have been injured by Intel’s alleged

¹³ Similarly, Plaintiffs’ allegations that Spectre and Meltdown posed a “significant security threat” underscore that, despite their complaints about the performance impact of the patches, no reasonable Plaintiff or putative class member would prefer a situation in which *no* patch was available to mitigate those exploits over one where a patch (albeit allegedly imperfect) was available. Indeed, the international standards endorsed by Congress provide that “[a] temporary or intermediary remediation that consists of a mitigation or workaround can be necessary in cases when a vulnerability poses a high risk to users. A non-comprehensive remediation that works in most scenarios can also be necessary in high-risk circumstances.” Ex. 13 (ISO 30111) at 10.

post-January 2018 conduct, and is inconsistent with the result reached in *Hauck* on indistinguishable facts. Thus, in differentiating time periods that may proceed from those that may not, where the Court presently demarcates only conduct before and after September 1, 2017, Order at 33, it should—if permitting any claims at all to survive—draw a similar line between conduct before and after January 2, 2018.¹⁴

Plaintiffs have acknowledged throughout this litigation that all the security vulnerabilities at issue in this action are “variants” of a single new “class of exploits” that was publicly and widely disclosed in January 2018. *E.g.*, 2AC ¶ 5; *compare* ECF 181 ¶ 5 (same); ECF 115 ¶¶ 6, 302-03 (same as to “class of attacks”). They also allege that further variants “are expected,” 2AC ¶ 8, and have said as much throughout. *See* ECF 115 ¶ 297 (noting “numerous new variants”). Plaintiffs similarly admit that the performance impact of the mitigation patches for that class of exploits has been publicly and widely disclosed. *E.g.*, 2AC ¶ 110.¹⁵ A consumer who buys after a new class of security vulnerabilities, and the implications of mitigations for those vulnerabilities, have been publicly and widely disclosed cannot plausibly claim to have been treated unfairly by the emergence of “expected” further variants (and related mitigations).

Plaintiffs’ claim that Intel has charged a “premium price” for its CPUs post-disclosure cannot serve as the necessary unifying conduct for all such purchasers. To the contrary, when Plaintiffs originally identified “five Named Plaintiffs [who] bought their computers *after* the security vulnerabilities were announced” in January 2018 (“and two Named Plaintiffs even bought

¹⁴ Spectre and Meltdown received widespread publicity starting on January 2, 2018; the first constituent suit in this MDL (*Garcia*, in the Northern District of California) was filed the next day.

¹⁵ In the context of the processing speed of contemporary CPUs, the Court has noted that an alleged “30% performance degradation” of this kind, which Plaintiffs characterize as “common,” 2AC ¶ 885, is “an infinitesimal change.” ECF 204 (3/29/21 Order) at 18 (citing *Hauck v. Advanced Micro Devices, Inc. (Hauck I)*, 2018 WL 5729234, at *9 (N.D. Cal. Oct. 29, 2018)).

new computers with Intel processors after filing their lawsuits” in this MDL), the Court expressly noted that fact in concluding that Plaintiffs had not plausibly alleged a diminution in value of, or overpayment for, their devices. ECF 178 (3/27/20 Order) at 12, 33; *see also id.* at 18 (noting that Plaintiffs could not recover without identifying what aspect of purchasers’ alleged bargain Intel did not meet). Consistent with the Court’s reasoning, Judge Koh held that a consumer who bought a device in January 2018, a few days after the Spectre and Meltdown vulnerabilities were “made public and discussed extensively in the press,” could not recover as a matter of law. *Hauck II*, 2019 WL 1493356, at *13. Judge Koh reached that decision notwithstanding those plaintiffs’ emphasis that Spectre was just “the tip of the iceberg,” with post-January 2018 variants applicable to AMD processors already identified and others expected. Ex. 14 (*Hauck* Am. Compl.) ¶¶ 163-64 (noting new variants disclosed in May 2018 and July 2018, including variants “successful in exploiting the defect in AMD CPUs”). And Judge Koh reached this conclusion even though the plaintiffs alleged that AMD “falsely stat[ed] that ‘there is a near zero risk to AMD processors’” even “following the public exposure of vulnerability to side-channel attacks” and did not “correct[] that false statement” until January 11, 2018—*after* all plaintiffs purchased their AMD processors. *Id.* ¶ 262(c). The Ninth Circuit affirmed, based on “the wide publicity” surrounding those vulnerabilities, as well as the facial implausibility of any suggestion that consumers believe their devices to be altogether invulnerable. *Hauck III*, 816 F. App’x at 43.

In response to the Court’s skepticism about purchasers “*after* the security vulnerabilities were announced,” ECF 178 (3/27/20 Order) at 12 (and likely with an eye to Judge Koh’s ruling in the indistinguishable context of *Hauck*), Plaintiffs swiftly dropped all five Named Plaintiffs who purchased devices after January 2018 from their subsequent amendments. *See generally* ECF 181, 2AC. Plaintiffs have never again identified a single person allegedly injured by Intel’s conduct

after disclosure of Spectre and Meltdown, and no such person possessing any claims for a purchase after that disclosure is a Named Plaintiff in this suit. Yet since the inception of this MDL, all three of Plaintiffs’ consolidated complaints have included substantially the same allegations regarding the period after January 2018—i.e., that new variant vulnerabilities have been discovered and further variants are expected, that consumers continue to pay undiminished prices for Intel processors, and so forth. ECF 115 ¶ 2, 245, 256, 266, 280-81, 283-93, 297, 303; ECF 181 ¶ 5, 8-9, 473, 543, 554, 571, 578, 614, 616; 2AC ¶ 599, 610, 627, 670, 672, 915. On those fundamentally unchanged allegations, the Court dismissed all claims twice before, and only now has the Court appeared to suggest that every single sale by Intel *even throughout the duration of this MDL* may be plausibly “unfair” or “unjust” (or even “unconscionable”).

Respectfully, extending the scope of this case to Intel’s alleged conduct *after* the widespread disclosure of Spectre and Meltdown in January 2018 cannot be squared with either the Court’s prior reasoning or the conclusion reached on indistinguishable facts in *Hauck*.¹⁶ Both this case and *Hauck* involve allegations that the defendant’s devices are susceptible not just to Spectre and/or Meltdown, but to ongoing vulnerability variants that post-date the January 2018 disclosure of this new class of vulnerabilities, and that the mitigations deployed cause unacceptable decreases in speed.¹⁷ Yet only Intel—after three rounds of briefing oriented around the historical Defects

¹⁶ Nor can that scope be squared with Plaintiffs’ own allegations that both the exploits and the performance impact of their mitigations have been widely known since January 2018. Likewise, as the seven remaining Named Plaintiffs all purchased *before* January 2018, none could have relied on, or been injured by, Intel’s alleged conduct after the embargo ended on January 2, 2018.

¹⁷ The *Hauck* plaintiffs claimed that AMD delayed disclosure of this new class of attacks, *see* Ex. 14 (*Hauck* Am. Compl.) ¶¶ 157, 163, including that AMD sat on knowledge of additional variants for nearly a year between June 2017 and May 2018. Those plaintiffs claimed performance impacts on AMD processors substantially identical to those claimed here, *see id.* ¶¶ 170-71 (alleging “ballpark figure of *five to 30 per cent slow down*” (emphasis in original)), and (as here) that the only true fix is a “total[] redesign” of AMD’s processors, *id.* ¶¶ 165-66, 174. And much like Plaintiffs here, the *Hauck* plaintiffs alleged that a malicious hack would be undetectable by

Theory now dismissed with prejudice—is unexpectedly threatened by an abrupt pivot to an Exploits Theory that not only treats as plausible claims dating to the Spectre and Meltdown embargo, but supposes that Intel *is still treating unfairly the buyers of every processor it continues to sell each day*, more than four years after the broad public disclosure of this new class of vulnerabilities.¹⁸

It is a basic tenet of our adjudicatory system to “endeavor to ensure that like cases reach like results.”¹⁹ That tenet is at risk here. Particularly where Plaintiffs have studiously refused to put forward any person who bought an Intel processor after January 2018, Intel respectfully requests that the Court—even if it permits claims to proceed regarding some portion of the period in 2017 when Intel, Google, AMD and others knew before the public about this new class of vulnerabilities—reconsider its decision opening the door to claims after January 2018.

II. IN THE ALTERNATIVE, THE COURT SHOULD CERTIFY THE ORDER FOR APPEAL.

If the Court declines to reconsider the issues identified above, and permits Plaintiffs to proceed under the Exploits Theory, the Court should certify the Order for interlocutory appeal pursuant to 28 U.S.C. § 1292(b), and, pursuant to Federal Rule of Appellate Procedure 5(a)(3), amend the Order to state the basis for certification. *See, e.g., Allied Prof'l. Ins. Co. v. Anglesey*, 2018 WL 6219920, at *3 (C.D. Cal. June 14, 2018) (“When a district court’s original order does

consumers. *Id.* ¶¶ 3, 157; *compare* 2AC ¶ 692. Meanwhile, as Plaintiffs’ own citations confirm, AMD processors are indisputably susceptible to other hardware vulnerabilities and variants to which Intel processors are not. *See* ECF 213 (Intel MTD 2AC) at 7 & n.5.

¹⁸ Notably, at oral argument, when the Court suggested that Intel might face liability, *at most*, with respect to “the consumers that purchased basically in the second or third quarter of 2017,” counsel for Plaintiffs initially agreed, before having second thoughts and quickly pivoting to suggest that such liability should be open-ended. Ex. 1 (12/9/21 Hr’g Tr.) 42.

¹⁹ William B. Rubenstein, *The Concept of Equality in Civil Procedure*, 23 Cardozo L. Rev. 1865, 1868 (May 2002).

not indicate whether the order is certified for interlocutory appeal, the ‘court may amend its order, either on its own or in response to a party’s motion, to include the required permission or statement.’ Fed. R. App. P. 5(a)(3).”).²⁰

A. The Court Should Certify Whether the Lack of a Misrepresentation, Physical Safety Hazard, or Breach of Warranty Precludes Stating a Plausible Claim of Unfairness Here.

Should the Court decline to reconsider and dismiss the Exploits Theory as barred by *Bardin* and the cases that follow its reasoning, the Court should certify the question of whether Plaintiffs may proceed with their product-based unfairness claim under the UCL, despite the lack of any misrepresentation, physical safety hazard, or breach of warranty. As discussed above, to state an unfair prong claim under the UCL, a plaintiff must allege a misrepresentation, a physical safety hazard, or a breach of warranty. These prerequisites flow from the California rule that a UCL unfair prong claim does not lie where a product functions as warranted, but nevertheless fails to meet the purchaser’s expectations because of a defect that manifested after the warranty period. *See, e.g., Clemens*, 534 F.3d at 1026-27 (dismissing UCL unfair prong claim because “the failure to disclose a defect that might, or might not, shorten the effective life span of an automobile part that functions precisely as warranted throughout the term of its express warranty cannot be characterized as causing a substantial injury to consumers, and accordingly does not constitute an unfair practice under the UCL”). The rationale for that rule applies equally—indeed, more—here, where Plaintiffs do not even allege that Intel warranted the CPUs would provide a specific speed

²⁰ Amending the Order to specify the issues certified and the basis for certification—including, if the Court so concludes, adding an express ruling that *Bardin* does not bar the surviving portion of Plaintiffs’ UCL claims—is also consistent with the Ninth Circuit’s guidance in *ICTSI Oregon, Inc. v. Int’l Longshore & Warehouse Union*, 22 F.4th 1125, 1132-33 (9th Cir. 2022), as it ensures that the issues presented for review are within the “four corners” of the order certified.

or performance, but nonetheless assert that Intel acted unfairly by not meeting Plaintiffs' expectations as to speed and performance.

This rule constitutes a “controlling issue,” as its resolution in Intel’s favor “could materially affect the outcome of [the] litigation.” *In re Cement Antitrust Litig. (MDL No. 296)*, 673 F.2d 1020, 1026 (9th Cir. 1981) (explaining “all that must be shown in order for a question to be ‘controlling’ is that resolution of the issue on appeal could materially affect the outcome of litigation in the district court”), *aff’d sub nom. Arizona v. Ash Grove Cement Co.*, 459 U.S. 1190 (1983). Applying California precedent restricting products-based unfairness claims to those asserting a misrepresentation, physical safety hazard, or breach of warranty would eliminate the UCL claim (and, by extension, the unjust enrichment claim). Dismissal of all remaining nationwide claims indisputably would “materially affect the outcome of litigation” here. *Id.*

Intel believes the rule in *Bardin* squarely applies here. The Exploits Theory (like Plaintiffs’ “Defects” theory) rests expressly on Plaintiffs’ claim of disappointed economic expectations for their devices, but does not allege any actionable misrepresentation (Order at 19–21), any physical safety hazard, or any breach of warranty. To the extent the Court disagrees, that disagreement necessarily demonstrates that reasonable jurists could disagree as to the scope of the rule. *See, e.g., Reese v. BP Expl. (Alaska) Inc.*, 643 F.3d 681, 688 (9th Cir. 2011) (noting “[a] substantial ground for difference of opinion exists where reasonable jurists might disagree on an issue’s resolution, not merely where they have already disagreed”).

Finally, this controlling issue of law could largely terminate this litigation if resolved in Intel’s favor, as it would eliminate the remaining nationwide claims. Therefore, its resolution is “likely to materially speed the termination of the litigation.” *Arthur*, 2012 WL 13047758, at *3; *see also Reese*, 643 F.3d at 688 (“[N]either § 1292(b)’s literal text nor controlling precedent

requires that the interlocutory appeal have a final, dispositive effect on the litigation, only that it ‘may materially advance’ the litigation.”).

B. The Court Should Certify Whether the Failure To Terminate an Embargo After a “Typical” Period States a Plausible Claim of Unfairness.

Should the Court decline to reconsider and dismiss the Exploits Theory as resting on an implausible allegation of embargo manipulation, the Court should certify the question of whether a plaintiff may base a plausible claim of unfairness on a bright-line rule regarding the “typical” length of an embargo.

This question presents a controlling issue here. All remaining Named Plaintiffs purchased during the period after the end of the allegedly “typical” 90-day embargo period but before the public disclosure of Spectre and Meltdown in January 2018. None could have been injured by any conduct on Intel’s part after January 2018 (such as Intel’s alleged misrepresentations that all manufacturers are affected by this new class of vulnerabilities). Their claims hinge entirely on Plaintiffs’ conclusory allegation that Intel “manipulated” the Spectre and Meltdown embargo (while continuing to sell and market its processors without revealing upcoming vulnerabilities). Thus, were a court to conclude that the mere assertion of an embargo period exceeding 90 days does not suffice to plausibly state a claim of unfair “manipulation,” “the case would be over.” *See Reese*, 643 F.3d at 688 (accepting certification of interlocutory appeal raising question of whether scienter could be plausibly inferred from facts alleged). Moreover, the issue is not merely controlling in this case, but threatens to have cascading negative implications if not reconsidered or certified. Tens of thousands of cybersecurity vulnerabilities are identified every year. The Court’s adoption of this new Exploits Theory on the bare and implausible allegations here puts every technology company evaluating such vulnerabilities at risk: Any time a mitigation is not ready within 90 days, the vendor must weigh premature disclosure (and the attendant risk to the

public) against the risk of class action exposure. If not reconsidered, the issue warrants certification.

As to the second requirement, both the district court and Ninth Circuit decisions in *Hauck* each rejected liability based on materially indistinguishable allegations that AMD failed to disclose Spectre and Meltdown. *Hauck II*, 2019 WL 1493356, at *11-15; *Hauck III*, 816 F. App'x at 42-43; see Ex. 14 (*Hauck* Am. Compl.) ¶¶ 157, 163, 165-74. Moreover, there are significant data security implications raised by the notion that, to avoid potential liability under the UCL, a vendor must disclose a vulnerability on Day 91 of an embargo—contrary to the coordinated vulnerability disclosure practices endorsed by the United States Government. Given the outcome in *Hauck*, as well as the countervailing public policy concerns with establishing a universal bright-line deadline to disclose security vulnerabilities, this issue at a minimum represents one “on which fair-minded jurists might reach contradictory conclusions,” such that it “may be certified for interlocutory appeal without first awaiting development of contradictory precedent.” *Reese*, 643 F.3d at 688. And because the extension of the embargo period beyond the allegedly “typical” 90 days is the linchpin on which the Named Plaintiffs’ claims turn, resolution of this issue is “likely to materially speed the termination of the litigation.” *Arthur*, 2012 WL 13047758, at *3.

CONCLUSION

The Court should grant Intel’s motion for reconsideration with respect to all issues addressed in this motion. In the alternative, Intel respectfully requests that the Court certify its Order for appeal pursuant to 28 U.S.C. § 1292(b).

DATED: February 23, 2022.

Respectfully submitted,

STOEL RIVES LLP

/s/ Steven T. Lovett

Steven T. Lovett, OSB No. 910701

steve.lovett@stoel.com

Rachel C. Lee, OSB No. 102944

rachel.lee@stoel.com

Telephone: 503.224.3380

WILLIAMS & CONNOLLY LLP

Daniel F. Katz (*pro hac vice*)

dkatz@wc.com

David S. Kurtzer-Ellenbogen (*pro hac vice*)

dkurtzer@wc.com

Telephone: 202.434.5000

Attorneys for Defendant Intel Corporation